GARY L. REBACK (SBN 100118)
greback@carrferrell.com
ROBERT J. YORIO (SBN 93178)
yorio@carrferrell.com
MARCUS H. YANG (SBN 273509)
myang@carrferrell.com
CARR & FERRELL *LLP*
120 Constitution Drive
Menlo Park, California 94025
Telephone: (650) 812-3400
Facsimile: (650) 812-3444

Attorneys for *Amicus Curiae*
CONSUMER WATCHDOG

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

GOOGLE INC.,

Defendant.

CASE NO. CV 12-04177 SI

**REVISED REPLY MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO THE ENTRY OF [PROPOSED] STIPULATED ORDER FOR PREMANENT INJUNCTION AND CIVIL PENALTY**

This reply memorandum addresses two issues raised by the parties' responsive briefs. The first goes to the adequacy of the remedy in the proposed order and, specifically, the extent to which Google continues to derive monetary benefit from its misconduct. An analysis of several of the conclusory statements from the government's brief, in the context of the technology at issue here, reveals that the deal between the parties does not even prevent Google from continuing to violate the Buzz Decree. Nor does it prevent Google from continuing to profit from the misconduct that it previously engaged in. The second issue involves the appropriate legal standard for review by the Court – specifically, whether the proposed consent decree needs to meet the "public interest" standard.

**A. The Parties' Proposed Order Permits Google to Continue to Profit from Its Misconduct.**

Consumer Watchdog's initial brief identified a number of serious deficiencies in the proposed order – the lack of a permanent injunction as contemplated by the complaint, a monetary penalty insufficient to satisfy either the objective of the statute or the stated objective of the Commission, and the defendant's outright denial of liability in the proposed order – and argued that the proposed order fails to satisfy the relevant legal standard. In reply, the government argued (among other things) that the remediation section of the proposed order "shields consumers from potential continued harm." Gov't Brief at 6. The government also asserted that Google "earned no more than $4 million from the alleged violation," Gov't Brief at 10, n.11, but provided no explanation of any kind for its calculation. *See* Bartley Decl. ¶ 6.

As we explained in our motion to file a reply brief, granted by the Court (Dkt. 25), when we examined these assertions in light of the "remediation" section in the proposed order, it became apparent that the order proposed to this Court does not eliminate or prevent "potential ongoing harm." Indeed, it permits Google to continue to profit from its wrongdoing indefinitely. Basically, the proposed remediation requires Google to "expire" the cookies it set in violation of the Buzz Decree, but permits Google to keep the data those cookies collected (including IP addresses) and to use that data in its ongoing business, thereby continuing to profit from its

misconduct. The government is either unaware of this result or has simply neglected to mention it to the Court, the press and the public.

We base this argument on our understanding of how tracking cookies generally work and on what Google said on its site about how it uses DoubleClick cookies – – up until a few days ago, when, after reading the Consumer Watchdog reply brief filed on October 18, Google changed its site to obscure the embarrassing admissions. In anticipation of this conduct, we printed the relevant portion of the site prior to Google's changes and attach it here as Exhibit A. *See How does Google use the DoubleClick cookie to serve ads*?, http://www.google.com/policies/privacy/ads (retrieved, as indicated on the document, on October 18, 2012 and attached as Exhibit A). In anticipation that Google may attempt to change the site back before the Court can detect the alterations, we attach a print out of the relevant portion of the site as of October 22, 2012 as Exhibit B (retrieved on October 22, 2012). Exhibit B is the page the user is now taken to if he now types "How does Google use the DoubleClick cookie to serve ads?" – – despite the fact that the page has been altered to eliminate that text.

- In violation of its obligations under the Buzz Decree, Google placed DoubleClick tracking cookies on Safari users' computers without permission in two different ways. The blog post of the FTC's (now former) chief technologist explained what Google did to place the cookies. *See* Ed Felton, *FTC Settles with Google over Cookie Control Override*, http://techatftc.wordpress.com/2012/08/09/google/. Basically, Google's DoubleClick server sent Safari users' computers small files, each containing a cookie ID (usually a string of letters and numbers).
- At the same time, DoubleClick created database entries on its systems corresponding to the cookie IDs. This fact was not stated, insofar as we can tell, in any of the FTC's written or oral explanations, either to the public or to this Court. Google's new privacy policy page now discloses this fact. *See* Exhibit C at 2. Undersigned counsel was not aware of the significance of this fact until he made inquiries after reading the government's filings in this case. As the Stanford researcher originally credited by the *Wall Street Journal* for revealing Google's Safari "hack" recently explained in a

presentation at The London School of Economics (posted to the web on October 12, 2012):

> [C]ookies don't collect anything. Cookies are just a little piece of information that gets saved in a browser. It's the website that collects things. And so sure, cookies don't collect personal information but because of their cookies, Google collected personal information.

LSE Safari-gate meeting transcript, http://www.privacysurgeon.org/blog/lse-safari-gate-meeting-transcript/ (at 24:21).

- The cookie ID was stored on each user's computer, but was sent back to DoubleClick with each HTTP request by the user's browser, and data about the user was recorded in the DoubleClick database. HTTP requests usually contain (among other things) the URL of the page requested, the URL of the page the user is currently on (the referrer URL), and the IP (Internet Protocol) address of the user. The IP address is simply a unique number assigned to each computer or device connected to the Internet. (If the user runs a search, the URL will contain the search terms.) All of this user data was recorded in the DoubleClick database, along with the cookie ID. *See* Exhibit A at 5.
- Because DoubleClick receives in one request both the URLs and the cookie ID, it can associate those URLs with the particular ID in its database. This permits Google to get a detailed picture of each user's web browsing and search activities. DoubleClick uses this information to serve targeted ads to the cookie ID when that cookie ID shows up on a site in Google's DoubleClick network. Safari's default privacy controls – which block third-party cookies (like DoubleClick's) by default – are intended to prevent this result. But Google created a workaround for this setting, which allowed Google to continue to set DoubleClick cookies, track users and serve those users targeted ads.

The "remediation" requirement in the Proposed Stipulated Consent Order only requires Google to "expire" the cookies it set on Safari browsers before February 15, 2012. The proposed order does **not** require Google to delete the data it collected against these cookie IDs (*i.e.*, the

data in Google's (DoubleClick's) databases). Nor does the proposed order impose any limits on what Google can do with this data. Google can and will use the data for profit on a going-forward basis.

By "expiring" the wrongfully placed cookies, Google can no longer associate particular user data in its database with a particular wrongfully placed cookie ID, as the "expired" IDs are no longer valid. The next time the user goes on DoubleClick, he will get a new cookie ID. However, his IP address will not likely change, and, as Google's FAQ site indicated before alteration (Exhibit A at 5), Google has already collected and stored IP addresses for the wrongfully-placed cookies. So, by referring to the user's IP address, Google can continue to use the wrongfully obtained data and track the user in the future and serve him targeted ads. In other words, using the IP address, Google can associate the user's new cookie ID with the wrongfully obtained data in its database.

The court will note that the Google FAQ site before October 18, 2012, merely listed IP addresses as one of the items of user information Google collected. *See* Exhibit A at 5. As indicated above, that page has been eliminated by Google. Now elsewhere on its site, Google describes IP addresses, gratuitously adding that "depending on the user's server, a different address may be assigned to the user by their service provider each time they connect to the Internet." Exhibit D at 2. While this is technically true, it so rarely happens that companies use IP addresses to associate different cookie IDs on the same machine across search sessions all the time.

It is common knowledge and common practice in the industry to use IP addresses and "referrer fields" (another item collected by Google cookies) to track internet users' browsing. *See* HTTP cookie, http://en.wikipedia.org/wiki/HTTP_cookie ("Tracking cookies may be used to track internet users' web browsing. This can also be done in part by using the IP address of the computer requesting the page or the referrer field of the HTTP request header, but cookies allow for greater precision.")

The proposed order does not prohibit Google from doing this. So the proposed order permits Google to go right on using improperly obtained user data for commercial purposes – –

including continuing to target advertising to the Safari users who received Google cookies improperly. The proposed order could prevent this result simply by requiring Google both to expire the cookies and to expunge all data collected from those cookies.

Moreover, even if (for whatever reason) Google is not using IP addresses to continue targeting the Safari users – – and cannot in the future (for whatever reason) associate the data entries in its database with particular cookie IDs (or even particular IP addresses), Google will still profit from the data it collected in violation of the Buzz Decree. More specifically, the kind of profile data Google collected can be used for profitable purposes other than targeting advertising to the particular users from whom data was initially collected. For example, analyzing a number of profiles helps Google to understand typical search patterns (for example, people who visit NYTimes.com are more likely to visit other newspaper sites in the same browsing session).

The wrongfully collected data, then, can still be used to target others (sometimes called "lookalikes") who exhibit similar behaviors. For example, if Google's wrongfully collected data shows that people in a particular browsing pattern (*e.g.*, tech blogs) are more likely to click on a particular ad (*e.g.*, an ad for Google's Chrome web browser), this information can be used to target ads at users who exhibit similar behavior in the future.

As Paragraph 50 of the Buzz Complaint alleges, Google collected and used – and, as we now know, continues to use – information about web-browsing activity from Safari users to whom it represented that it would not collect such information. According to the Buzz Complaint, this continuing conduct violates Part 1(A) of the Buzz Decree – misrepresenting the extent to which users may exercise control over the collection or use of covered information. *See* Safari Complaint at ¶ 51. Again, the proposed order could prevent this result simply by requiring Google to expunge the wrongfully collected data from its database. If Google (or the government) contends that it cannot identify the data fields of affected Safari users with particularity, Google should be required to expunge its entire database of Safari users and start over. After all, according to the declaration supporting the government brief, "[t]he FTC only included or excluded relief based on what it determined to be in the best interests of consumers."

Permitting Google to settle this case without expunging wrongfully collected data runs afoul of the position taken by the FTC in a prior Google investigation. As we noted in our initial brief, the FTC closed down its investigation of the Wi-Spy scandal only after Google publicly stated its "intention to delete the inadvertently collected data as soon as possible" and gave "assurances to the FTC that the company ha[d] not used and [would] not use any of the [wrongfully collected data] in any Google product or service, now or in the future." The FTC's Director of the Bureau of Consumer Protection based the Commission's decision to close the investigation squarely on this representation: "This assurance is critical to mitigate the potential harm to consumers from the collection of payload data," he wrote. *See* Consumer Watchdog Initial Memorandum at 3.

Perhaps, in the Court's discretion, the Court may wish to defer to the FTC's judgment – however suspect and unsupported – as to the propriety of an order intended to deter Google from future misconduct. But it is hard for us to imagine that the Court would approve a settlement that does not even stop Google from continuing the very misconduct alleged in the complaint. Under any legal standard, the proposed remedy is simply inadequate.

We are mystified as to why the government did not point out to the Court Google's ability to continue to use improperly-collected data in the future. Surely, this is something the Court would like to know in evaluating the proposed settlement. We believe the government should have given the Court the technical background we have provided in this brief. Indeed, we do not know which is worse – the government's failure to stop Google's continuing misconduct or the government's failure to disclose to the public and this Court that Google will continue to use the improperly collected data.

The government's brief claims that Google "earned no more than $4 million from the alleged violation" and that the penalty "was many times the upper-bound of what the FTC estimates the company earned from the alleged violation." Gov't Brief at 9-10 and n. 11. The brief also claims difficulty in making a "per violation" calculation because "only a small subset of Safari users viewed the misrepresentation." The brief gives no indication that the government included or even understood that Google would continue to profit from its misconduct.

In any case, third party analysts had far less difficulty calculating the appropriate penalty than the government now claims to. According to the FTC, there are 190 million Safari users. [1] Also, according to the FTC, every Safari user "probably received a DoubleClick tracking cookie during the relevant time period." [2] If even one-tenth of one percent of Safari users saw the misrepresentation, the statutory penalty would exceed $3 billion. An independent analyst, using the most conservative assumptions possible, estimated the statutory penalty at $8 billion.[3] Surely the government could have made a realistic calculation of how many Safari users saw the misrepresentation had it bothered to compel discovery from Google

Of course, this just represents a calculation of the statutory penalties. As the government points out, the issue for this Court is not simply the size of the penalty under the statute, but rather the benefit obtained by Google from its misconduct (and the consequent harm to consumers). The deterrent effect from the settlement, according to the government, flows from the government's unsupported assertion that the negotiated penalty exceeds the government's estimate of what Google earned from its misconduct.

But, in making an estimate of what Google earned from its misconduct, there is no reason to limit the calculation to users who saw the misrepresentation. Harm to users comes less from the fact that people were falsely assured by Google that leaving the Safari settings unchanged would prevent them from being tracked than it does from the circumvention of users' privacy settings in the first place.

Millions upon millions of users had their browser settings overridden as a result of Google's intentional misconduct - - regardless of whether they saw Google's notice. These users exercised a choice about allowing third parties to track them, and Google intentionally

---

[1] FTC Google Twitter Chat Transcript http://www.ftc.gov/opa/socialmedia/twitterchats/120809googletwtchat.pdf.

[2] Ed Felton, FTC Settles with Google Over Cookie Control Override http://techatftc.wordpress.com/2012/08/09/google/.

[3] Elizabeth H. Johnson, High Stakes, http://www.poynerspruill.com/publications/Pages/GoogleAllegedCircumventionSafariPrivacySettings.aspx.

disregarded that choice. The reason Google engaged in this conduct was to circumvent controls that were preventing it from profiling people, and selling ads based on those profiles.

The benefit Google reaped from this conduct is not limited to monetizing the data collected from users who saw the misrepresentation. Neither the government nor Google could possibly argue this. The benefit to Google comes from its having collected data from estimated 190 million users who had chosen not to have their data collected by third parties.

The government has not given this Court any insight into how it made its calculations. From what is available in the government's brief, and from Google's site (before alteration) and from other sources on the web, we believe we have shown: (1) that Google has continued to profit from its misconduct by tracking Safari users whose cookies were "expired"; (2) that Google can (and does) continue to profit from the data it improperly collected by profiling other users with this data and otherwise employing the improperly collected data in its services; and (3) that the benefit to Google from its misconduct is not limited to users who saw Google's misrepresentations. We cannot more precisely quantify the amount of Google's monetary benefit without taking discovery of Google - - something the government should have done. If the Court seeks more precise calculations from us, we ask that the court permit us to take relevant discovery.

Issues regarding web privacy involve technical details that make blatant and intrusive privacy violations seem academic and rather innocuous. A comparison to real world privacy violations might be helpful to explain the consequences of approving the proposed order.

Suppose a Peeping Tom were loose in a residential neighborhood. The Peeping Tom, once apprehended by the authorities, was shown to have both leered into people's bedrooms and bathrooms at night and to have taken pictures of what he saw. The government now proposes to settle the case with the Peeping Tom by preventing him from leering into people's homes in the future. But the government proposes to let the Peeping Tom keep all the invasive pictures he has taken, and publish them in a book for profit. At very most (under the provisions here) the government would require the Peeping Tom to delete street addresses and to obscure the facial characteristics of his victims so that they cannot be identified easily – and he could then go ahead

with publication. Ordinary people would find it difficult to understand such a result under any legal standard.

**B. The Court Should Apply the Public Interest Standard in Evaluating FTC Settlements.**

The parties would have this Court be the first in the nation (of which we are aware) to hold that consent settlements involving the Federal Trade Commission need not be in the public interest. Only a few months ago, when the FTC volunteered in federal court that its consent settlements had to meet the public interest standard, it made no effort to limit that admission to any particular federal circuit. We find it hard to imagine that the Commission could now (or ever) take the position that it did not have to act in the public interest or otherwise satisfy the public interest standard.

We are aware, of course, that this Court and others in this circuit have evaluated consent decrees involving government agencies under a legal standard that does not expressly include the public interest requirement. But the FTC Act, under which this suit is brought, has its own legislative history. As we explain below, the Act was amended expressly to empower the Commission to protect the public, and, hence, we believe that the Commission's actions under § 5(l) of the Act must satisfy the public interest standard. The government seems to recognize the point. In *Circa Direct*, the FTC conceded that "a district court reviews a proposed consent decree to ensure it . . . serves the public interest as articulated in the underlying statute." March 14, 2012 FTC submission at 2. The government in this case quotes that same passage for precisely the same point. *See* Gov't Brief at 3, n.4.

The government brings this case under § 5(l) of the FTC Act. That section was amended in 1938 expressly to give the FTC the responsibility to protect the public interest at large. *See* S. Rep. No. 75-221 at 2 (1937). Prior to the amendment, the Commission was empowered only to act in "private controversies" among competitors. Thus, the amendment empowered the Commission to stop "exploitation and deception of the public" even without injury to competitors of the defendant. S. Rep. No. 75-221 at 3 (1937). And the Commission was given

the power to restrain unfair acts if the restraint "be in the public interest." S. Rep. No. 75-221 at 3-4 (1937).

Similarly, the House Report stated that the amendments to Section 5 empowered the Commission to prevent acts "which injuriously affect the general public," and, specifically, "the consumer." *See*. H. R. Rep. No. 75-1613 at 3 (1937). Moreover, as we have noted, the Seventh Circuit observed decades ago that the Commission "unlike a private litigant, must act in furtherance of the public interest." *Johnson Prods. Co. v. F.T.C.*, 549 F.2d 35, 38 (7th Cir. 1977).

Many of our arguments go to the issue of whether the proposed settlement is "adequate." But, as both we and the parties have noted in briefing, the "public interest" standard is broader and far less deferential than the more limited "fair, reasonable, and adequate" requirement. In any case, we believe that the parties' proposed order fails to meet the appropriate legal standard.

Dated: October 23, 2012

Respectfully submitted,

/s/ Gary L. Reback

Gary L. Reback, Of Counsel
Carr & Ferrell LLP

Attorneys for *Amicus Curiae*
Consumer Watchdog

**EXHIBIT A**

Google

## Policies & Principles

# Advertising privacy FAQ



## How does Google protect my privacy when it comes to advertising?

We make protecting privacy a priority by being clear about what information we collect and how we will use the information to show relevant ads. We also make it easy for you to view, manage, and opt out of personalized ads on a variety of services ranging from Google properties like search, third party AdSense sites, and Google applications or clients. Of course, we will not sell or share with third parties your personally identifying information from ad serving cookies without your consent.

## What information does Google use to serve me ads?

We serve ads through our AdWords program on our own websites, as well as on the Google Display Network. We also serve ads through our AdSense and AdMob programs on

third-party partner sites and services (such as applications and other clients). We use a variety of methods to deliver ads that are relevant.

For the Google Display Network and AdMob network, we serve ads based on the content of sites you've viewed or the application you're using on your device and may also use other partner data to target ads. For example, if you visit a gardening site, ads on that site may be related to gardening. In addition, we may serve ads based on your interests. As you browse Google sites or websites that have partnered with us or use and download applications on your device, Google may place cookies or anonymous identifiers (see more on anonymous identifiers below) in your browser or on your device to understand the types of pages visited, content that you viewed or applications on your mobile device. Based on this information and/or anonymized partner data, Google associates your cookies or anonymous identifiers with relevant interest categories and uses these categories to show interest-based ads. For example, if you frequently visit travel websites, Google may show more ads related to travel. Or, if you download a golf application, Google may show you ads related to golf. Google may also show you ads related to the content of sites in your recent browsing history. Google can also use the types of pages that you have visited, content that you have viewed, or applications on your device to infer demographics like your gender and age category. For example, if the sites that you visit and applications you download have a majority of female visitors (based on aggregated survey data on site visitation or application usage), we may associate your cookies and anonymous identifiers with the female demographic category.

In addition to ads based on interest categories, Google allows advertisers (including Google) to show you ads based on your previous interactions online or in applications, such as visits to advertisers' websites or applications. For example, someone who visited the website or shopping application of an online sporting goods store can later receive ads about special offers from that store.

Google will not associate sensitive interest categories with your cookies or anonymous identifiers (such as those based on race, religion, sexual orientation, health, or sensitive financial categories), and will not use such categories when showing you interest-based ads.

## What information is used to personalize ads on Google search, Gmail, and other Google properties?

When you search for something on Google without being signed in to your Google Account, the search results page shows results and ads that match your current search terms and

location. If we think that the ads will be more relevant, we may also use recent searches for related topics and ads that you've clicked to decide which ads to show.

When you are signed in to your Google Account, we may use additional information to decide which ads to show. For example, we may use a recent previous search if we think the searches may be related, like a search for "New York" followed by a search for "hotels" – this can indicate that you want to find out about hotels in New York. We only use recent searches because it usually doesn't make sense to draw connections between searches that are very far apart in time.

Another way we can personalize ads on search is by using your Google Web History. For example, if you recently clicked a search result for a surfing website, and then searched for "vacations," this can indicate that you're interested in vacation destinations where you can surf, and you may see ads for surfing vacations.

Additionally, we may use information that you tell us about yourself to personalize ads on search. For instance, certain products may give you the opportunity to tell us that you really like a particular retailer or brand and we can use that information later to show you ads for merchants and products & services that we think you might like.

In Gmail, most of the ads we show appear next to an open email message and match the contents of your email. When we personalize ads, we display ads based on the contents of all your emails. For example, if you've recently received lots of messages about photography or cameras, we might show you a deal from a local camera store.

Not all ads are personalized to you on Google search, Gmail, and other Google properties. We personalize ads only when we think the additional information improves the ad selection for you.

## What information does YouTube use to serve me interest-based ads?

Using the DoubleClick cookie, YouTube also displays interest-based advertising to show relevant ads on its site. The interest categories are determined by your visits to websites that use our AdSense program, as well as by the videos you search for, prefer to watch, or actions you take (such as uploading) on YouTube. The DoubleClick cookie associates your browser with relevant interest categories and uses these categories to show interest-based ads. We do not combine personally identifiable information from your YouTube account or Google

account with the cookie data used to serve interest-based advertising without your consent. To learn more, see YouTube Advertising and You.

## How do I edit my ads preferences for interest-based advertising?

Interest and demographic categories are based on visits to sites in the Google Display Network or other services or applications you use or download. Using the Ads Preferences Manager for browsers, you can edit your ads preferences in browsers by adding interest categories that are relevant to you. Using the Ads Preferences Manager for browsers and Ads Preferences Manager for applications, you can remove any interest categories that don't apply and Google will no longer use them for showing you interest-based ads. You can also change which demographic categories are associated with your cookies or anonymous identifiers. When you edit your ads preferences, your new settings may not take immediate effect, since it takes time for the change to be processed in our systems.

## How do I opt out of interest-based advertising?

If you prefer not to receive interest-based advertising in web browsers, you can always click the "Opt out" button on the Ads Preferences Manager. When you are accessing the web through a web browser, Google also offers a number of options to permanently save your opt-out settings in your browser. After you opt out, Google will not collect interest category information and you will not receive interest-based ads via Google when accessing the web through a web browser. You will still see the same number of ads as before, and Google may still show relevant ads based on the content of a web page, or other non-personal information. For example, if you visit a gardening site, Google can determine the content of the site and may automatically show ads related to gardening to all visitors without using a cookie. Additionally, whenever we serve an ad on Google search or on the sites of our AdSense for search partners, the ads which are displayed may still be based on the search terms you enter.

If you prefer not to receive interest-based advertising in applications and other clients that use anonymous identifiers, you can always opt out using the appropriate preferences manager.

Read more about opting out of interest-based advertising in applications and other clients.

## What is the Ads Preferences Manager?

The Ads Preferences Manager is a Google site where you can manage settings associated with the ads you see. Our goal is to provide you with transparency and choice about the ads we show you.

- For Google search and Gmail, we explain why you got specific ads, let you block ads from websites you aren't interested in, and opt out of seeing personalized ads on search results pages and in Gmail.
- For websites that have partnered with Google to show AdWords ads, we show you a list of the interests we associate with you which may affect the ads you see on those websites. We also let you add or delete interests from that list and opt out of seeing ads based on inferred interests or demographics.

## How does Google use the DoubleClick cookie to serve ads?

A cookie is a snippet of text that is sent from a website's servers and stored on a web browser. Like most websites and search engines, Google uses cookies in order to provide a better user experience and to serve relevant ads.

Google uses the DoubleClick cookie on AdSense sites, partner sites and certain Google services to serve more relevant ads across the web and limit the number of times a given ad is shown to you. When you visit a website, view an ad, or click an ad supported by Google's advertising services, we may set a cookie on your browser. This advertising cookie will appear in your browser as coming from the domain "doubleclick.net" or from the domain of the site you are visiting.

When the cookie is set on your browser, it allows Google to gather information about your browser's interaction with a given ad. This information gets recorded in a log that looks something like this:

```
time: 06/Aug/2008 12:01:32
ad_placement_id: 105
ad_id: 1003
userid: 0000000000000001
client_ip: 123.45.67.89
referral_url: "http://youtube.com/categories"
```

The "time" field reflects the time the ad was displayed. The "ad placement id" and "ad id" identify the advertising campaign and the specific ad served. The "userid" is the display ad

cookie that identifies the browser. The "client IP" reflects the user's Internet Protocol (IP) address. A "referral URL" indicates the URL of the page where the ad was served. Our logs also record whether a user's browser clicks or interacts with an ad.

This information helps Google deliver ads that are relevant to your interests, control the number of times you see a given ad, and measure the effectiveness of ad campaigns. Anyone who prefers not to see ads with this level of relevance can opt out. This opt-out will be specific only to the browser that you are using when you click the "Opt out" button.

## What is an anonymous identifier and how is it used in ad serving?

To serve ads in services where cookie technology may not be available (for example, in applications and other clients), we may use anonymous identifiers. To serve ads that are relevant and tailored to your interests, we may use information about your activity in these services as well as non-personally identifying information, such as demographic data.

Mobile applications may have access to your device identifier and may pass it to Google when you use an application that displays Google AdSense or AdMob ads. Whether or not we receive your device identifier, we only associate information directly with anonymous identifiers, not with device identifiers themselves. In cases where we receive your device identifier, an anonymous identifier is created in association with your device. This allows you full control, because unlike a device identifier that you cannot change or delete, you can choose to reset or disable anonymous identifiers at any time.

## How does Google use cookies for Google Analytics?

Google Analytics is Google's free web analytics tool that helps website owners understand how their visitors engage with their website. Google Analytics collects information anonymously, and much like examining footprints in sand, it reports website trends without identifying individual visitors. Analytics uses its own set of cookies to track visitor interactions. These cookies are used to store information, such as what time the current visit occurred, whether the visitor has been to the site before, and what site referred the visitor to the web page. Google Analytics customers can view a variety of reports about how visitors interact with their website so they can improve their website and how people find it. A different set of cookies is used for each website, and visitors are not tracked across multiple sites. Analytics customers are obliged to notify users of their use of analytics software. To disable this type of

cookie, some browsers will indicate when a cookie is being sent and allow you to decline cookies on a case-by-case basis. In addition to declining cookies, you can also install the Google Analytics Opt-out Add-on in your browser, which prevents Google Analytics from collecting information about your website visits.

For customers that have enabled the Remarketing with Google Analytics feature, the third-party DoubleClick cookie is used to enable remarketing for products like AdWords on the Google Display Network. To manage your settings for this cookie and opt-out of this feature, visit the Ads Preferences Manager.

Learn more about the Google Analytics Opt-out Browser Add-on and other Google Analytics privacy information.

## How does Google use cookies for other conversion tracking?

Beyond Google Analytics and DoubleClick cookies, Google uses cookies to help businesses that buy ads from Google determine how many people who click their ads end up purchasing their products. The conversion tracking cookie is set on your browser only when you click an ad delivered by Google where the advertiser has opted in to conversion tracking. These cookies expire within 30 days and do not contain information that can identify you personally. If this cookie has not yet expired when you visit certain pages of the advertiser's website, Google and the advertiser will be able to tell that you clicked the ad and proceeded to that page. Each advertiser gets a different cookie, so no cookie can be tracked across advertiser websites. If you want to disable conversion tracking cookies, you can set your browser to block cookies from the googleadservices.com domain.

Additionally, due to the current lack of per-domain cookie settings in iOS and Android mobile browsers, you must disable all cookies in order to opt out of mobile conversion tracking.

## How do I edit my ads preferences for applications and other clients?

You can use the Ads Preferences Manager for applications to edit associated interest categories, reset your ad preferences, or opt out of interest-based ads on your mobile device.

To change your preferences, simply follow the instructions below for your mobile device.

### Android

1. Open *Play Store* on your device
2. Press *Menu* and select *Settings*

### iOS

1. Download the Google Search app or scan the QR code above using your mobile device
2. Open the *Settings* page of the downloaded Google Search app

Your mobile applications ads preferences may also be applied to "Ads by Google" within your web browser and vice versa. To manage your ads preferences for "Ads by Google" you see within browsers, visit the Ads Preferences Manager for browsers.

**EXHIBIT B**

Google

## Policies & Principles

# FAQ



## How does Google protect my privacy?

At Google, we are keenly aware of the trust our users place in us, and our responsibility to protect their privacy. We believe transparency and choice are the foundations of privacy. To help you make informed decisions about your own privacy, we work to let you know what information we collect when you use our products and services and how we use that information to improve your service. We also work to give you meaningful choices when possible about the information you provide to Google and to others. We encourage you to watch our videos, read our privacy policy and consult our Help Centers to find out more about privacy at Google.

## Why does Google store search engine logs data?

We store this data for a number of reasons. Most importantly, we store data to improve our search results and to maintain the security of our systems. Analyzing logs data helps our engineers both improve your search quality and build helpful innovative services. Take the example of Google Spell Checker. Google's spell checking software automatically looks at a user's query and checks to see if that user is using the most common version of the word's spelling. If we calculate a user is likely to get more relevant search results with an alternative

spelling, we'll ask "Did you mean: (more common spelling)?" In order to provide this service, we study the data in our logs. Logs data also helps us improve our search results. If we know that users are clicking on the #1 result, we know we're probably doing something right, and if they're hitting next page or reformulating their query, we're probably doing something wrong. In addition, logs data helps us prevent against fraud and other abuses, like phishing, scripting attacks, and spam, including query click spam and ads click spam.

## Why are search engine logs kept before being anonymized?

We strike a reasonable balance between the competing pressures we face, such as the privacy of our users, the security of our systems and the need for innovation. We believe anonymizing IP addresses after 9 months and cookies in our search engine logs after 18 months strikes the right balance.

## How can I remove information about myself from Google's search results?

Like all search engines, Google is a reflection of the content and information publicly available on the web. Search engines do not have the ability to remove content directly from the web, so removing search results from Google or another search engine leaves the underlying content unaffected. If you want to remove something from the web, you should contact the webmaster of the site and ask him or her to make a change. Once the content has been removed and Google's search engine crawl has visited the page again, the information will no longer appear in Google's search results. If you have an urgent removal request, you can also visit our help page for more information.

## Does Google use cookies?

Yes, like most websites and search engines, Google uses cookies to improve your experience and to provide services and advertising. Cookies help us keep a record of your preferences, like whether you want your search results in English or French, or if you use our SafeSearch filter. Without cookies, Google wouldn't be able to remember what different people like. We also use cookies to provide advertising more relevant to your interests.

We've been told most users don't want to re-set their computers every time they log on. If you

don't want to receive cookies you can change your browsers to notify you when cookies are sent and then refuse cookies from certain websites (or altogether). You can also delete cookies from your browser. Google's search engine does work without cookies, but you will lose some functionality if you choose to disable cookies.

## What happens when different privacy laws in different countries conflict?

Many countries approach privacy issues differently and there is no consistent global standard on which all countries agree. Google's privacy policy is designed to be a single, clear, global statement of our approach to privacy, and our privacy practices under it are designed to meet applicable law around the world.

## How often are you asked by governments to provide data on users?

Like other technology and communications companies, we receive requests from government agencies around the world to provide information about users of our services and products. To help increase transparency about these requests we have created the Government Requests Tool, which shows the number of requests that we have received that relate primarily to criminal investigations. For more information about the tool and the nature of these requests, please check the Government Requests Tool FAQ.

## How can I contact Google if I have a privacy question or complaint?

You can contact us any time through our privacy contact form. If you prefer, you can also write to:

Privacy Matters
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View, California, 94043
USA

**EXHIBT C**

Google

## Policies & Principles

# Privacy Policy

Last modified: July 27, 2012 (view archived versions)

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us.

### Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful or the people who matter most to you online.

We collect information in two ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name,

email address, telephone number or credit card. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.

- **Information we get from your use of our services.** We may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes:

  - **Device information**

    We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

  - **Log information**

    When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include:

    - details of how you used our service, such as your search queries.
    - telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
    - Internet protocol address.
    - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
    - cookies that may uniquely identify your browser or your Google Account.

  - **Location information**

    When you use a location-enabled Google service, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

  - **Unique application numbers**

Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

  We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

- **Cookies and anonymous identifiers**

  We use various technologies to collect and store information when you visit a Google service, and this may include sending one or more cookies or anonymous identifiers to your device. We also use cookies and anonymous identifiers when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites.

## How we use information we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.

We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

When you contact Google, we may keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer.

When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

## Transparency and choice

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and control certain types of information tied to your Google Account by using Google Dashboard.
- View and edit your ads preferences, such as which categories might interest you, using the Ads Preferences Manager. You can also opt out of certain Google advertising services here.
- Use our editor to see and adjust how your Google Profile appears to particular individuals.
- Control who you share information with.
- Take information out of many of our services.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.

## Information you share

Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services

provide you with different options on sharing and removing your content.

## Accessing and updating your personal information

Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes).

Where we can provide information access and correction, we will do so for free, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

## Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances apply:

- **With your consent**

  We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

  - view statistics regarding your account, like statistics regarding applications you

install.
- change your account password.
- suspend or terminate your account access.
- access or retain information stored as part of your account.
- receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
- restrict your ability to delete or edit information or privacy settings.

Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

  We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

- **For legal reasons**

  We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

  - meet any applicable law, regulation, legal process or enforceable governmental request.
  - enforce applicable Terms of Service, including investigation of potential violations.
  - detect, prevent, or otherwise address fraud, security or technical issues.
  - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

## Information security

We work hard to protect Google and our users from unauthorized access to or unauthorized

alteration, disclosure or destruction of information we hold. In particular:

- We encrypt many of our services using SSL.
- We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

## Application

Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.

## Enforcement

We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

## Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior

versions of this Privacy Policy in an archive for your review.

## Specific product practices

The following notices explain specific privacy practices with respect to certain Google products and services that you may use:

- Chrome and Chrome OS
- Books
- Wallet
- Fiber

**EXHIBIT D**

Google

## Policies & Principles

# Key terms



## Personal information

This is information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google.

## Google Account

You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address and a password). This account information will be used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or terminate your account at any time through your Google Account settings.

## Cookie

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognize

your browser. Cookies may store user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies.

## Anonymous identifier

An anonymous identifier is a random string of characters that is used for the same purposes as a cookie on platforms, including certain mobile devices, where cookie technology is not available.

## IP address

Every computer connected to the Internet is assigned a unique number known as an Internet protocol (IP) address. Since these numbers are usually assigned in country-based blocks, an IP address can often be used to identify the country from which a computer is connecting to the Internet.

## Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
- `25/Mar/2003 10:15:32` is the date and time of the query;
- `http://www.google.com/search?q=cars` is the requested URL, including the search query;
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used; and

- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to the user the next time s/he visits Google from that particular computer).

## Sensitive personal information

This is a particular category of personal information relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality.

## Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually identifiable user.

## Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking activity on websites, or when emails are opened or accessed, and is often used in combination with cookies.